**Task 2**

The idea behind PRF is that given a key and an input of size n, it should return an output of same size which looks completely random to an polynomial time distinguisher. We use the PRG as constructed before to construct the PRF. This will be used as our encryption function when we construct CPA secure encryption schemes. Now, how can PRFs exist? I mean, it seems amazing that something that seems random is deterministic and can be decrypted given the key. The answer lies in the algorithm given below.

**Build Algorithm**

PRF Theorem: Suppose that one way functions exist and PRG exists, then there exists a secure PRF collection $\{f_s\}_{s\in\{0,1\}^n}$ such that for every $s \in \{0,1\}^n$, $f_s$ maps $\{0,1\}^n$ to $\{0,1\}^n$.

**Proof**

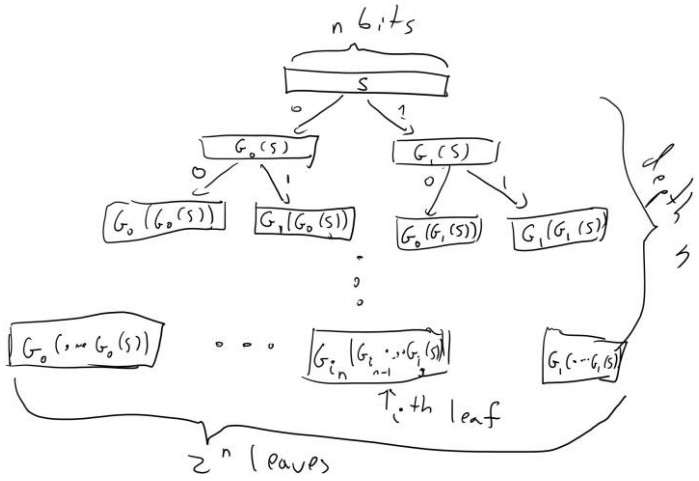
If the PRG Conjecture is true then in particular by the length extension theorem there exists a PRG $G : \{0,1\}^n \to \{0,1\}$ that maps n bits into 2n.

Now, lets denote the first n bits by $G_0(s)$ and last n bits by $G_1(s)$.

For $i \in \{0,1\}^n$, we define $f_s(i)$ as

$$G_{i_n}(G_{i_{n-1}}(\cdots G_{i_1}(s))).$$

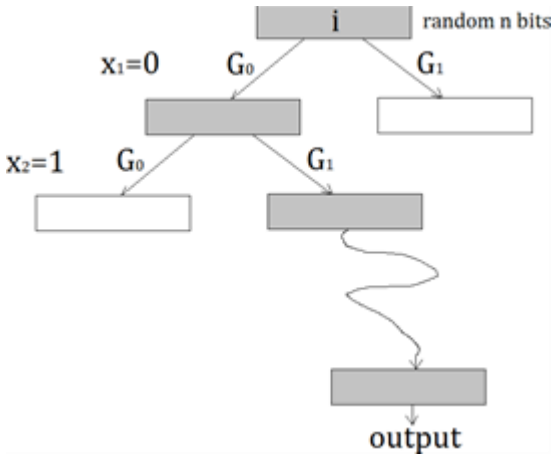
It can be easily replresented by a tree.




Hence, we see that to evaluate fs(i), we must evaluate the pseudorandom generator n times if the length of the input is n. Therefore, if the PRG is efficiently computable than so is PRF. Hence, we just need to prove that the given construction is secure.

We can rewrite what we must prove as follows.

Given an adversary $A$ that can distinguish in time $T$ a black box for $f_s(\ )$ from a black-box for a random function with advantage $\epsilon$, we need to come up withan adversary $D$ that can distinguish in time $poly(T)$ an input of the form $G(s)$ (where $s$ is random in $\{0,1\}^n$) from an input of the form $y$ where $y$ is random in $\{0,1\}^{2n}$ with bias at least $\epsilon/poly(T)$.




**Proof:** Assume for the purpose of contradiction that $\{F_n\}_{n\in\mathbb{N}}$ is not PRG. Then there exists a non-uniform PPT oracle adversary $A$ that can distinguish $\{F_n\}$ from $\{R_n\}$. Where Rn is truly random function.

We use hybrid argument. Define $H_i(i = 0, 1, \cdots, n)$ in the following way: Let $H_i$ be a full binary tree of depth $n$ where the nodes of levels 0 to $i$ are truly random values, and the levels $i+1$ to nare constructed by $G_0$ and $G_1$. Then we have $H_0 \equiv F_n$ and $H_n \equiv R_n$.
Since $A$ that can distinguish $H_0$ from $H_n$, by hybrid argument, there exists $j \in \{0, 1, \cdots, n-1\}$
such that $A$ can distinguish $H_j$ from $H_{j+1}$.

Next, we need to use hybrid argument again. Note that $A$ is PPT, so there are only poly($n$) nodes in the $j^{th}$ level of the tree that have been visited by $A$. Denote all the nodes by $v_1, v_2, \cdots, v_t$, where $t$ = poly($n$). We construct $H_{j,i}(i = 0, 1, \cdots, t)$ as follows: Let $H_{j,i}$ be a full binary tree of depth $n$ where the nodes of levels 0 to $j$ are random, the sons of nodes $v_1, v_2, \cdots, v_i$ are random,and all the rest nodes are constructed by $G_0$ and $G_1$. We have $H_{j,0} \equiv H_j$. Further, $H_{j,t}$ and $H_{j+1}$are equivalent for $A$ since the different nodes between $H_{j,t}$ and $H_{j+1}$ are not visited by $A$. Thus,$A$ that can distinguish $H_{j,0}$ from $H_{j,t}$. By hybrid argument, there exists $k \in \{0, 1, \cdots, t-1\}$ such that $A$ can distinguish $H_{j,k}$ from $H_{j,k+1}$.
Now we are ready to construct an adversary $B : \{0,1\}^{2n} \to \{0,1\}$ where the input $T$ could be either from $U_{2n}$ or $G(U_n)$: Construct a full binary tree of depth $n$ where the nodes of levels 0 to$j$ are random, the sons of nodes $v_1, v_2, \cdots, v_k$ are random, the left son of node $v_{k+1}$ is the first $n$bits of $T$, the right son of node $v_{k+1}$ is the last $n$ bits of $T$, and all the rest nodes are constructedby $G_0$ and $G_1$. Take this binary tree as the input of $A$, then we have

- if $T$ is from $U_{2n}$, then $A$'s input is from $H_{j,k+1}$;
- if $T$ is from $G(U_n)$, then $A$'s input is from $H_{j,k}$.

Since $A$ can distinguish $H_{j,k}$ from $H_{j,k+1}$, $A$ can distinguish from $U_{2n}$ and $G(U_n)$. Contradiction to the fact that $G$ is a PRG.